IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LEON STAMBLER,	§	
	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. 2:08-cv-204
	§	
JPMORGAN CHASE & CO., et al,	§	**JURY TRIAL DEMANDED**
	§	
Defendants.	§	
	§	

JPMORGAN CHASE & CO. AND JPMORGAN CHASE BANK, NATIONAL ASSOCIATION'S MOTION TO DISMISS BASED ON THE PRECLUSIVE EFFECT OF THE DELAWARE NON-INFRINGEMENT JUDGMENT

Eight years ago, the plaintiff Leon Stambler ("Stambler") brought suit against five companies in the U.S. District Court for the District of Delaware for alleged infringement of U.S. Patent No. 5,974,148 ("the '148 Patent") and U.S. Patent No. 5,793,302 ("the '302 Patent") (Exhibits A and B, respectively)[1] based on their use of an industry standard for secure Internet communications called Secure Sockets Layer 3.0 ("SSL"). That case went to trial, a jury determined that SSL did not infringe, and the Federal Circuit affirmed on appeal. Nonetheless, Stambler's Infringement Contentions in this case show that he is intent on trying to re-litigate before this Court the issue of whether SSL infringes these same two patents. In his Infringement Contentions, Stambler charges that the funds transfer services of JPMorgan Chase & Co and JPMorgan Chase Bank, National Association (collectively, "JPMorgan"), and specifically its use of SSL to ensure secure communications, infringe the '302 and '148 Patents. Because the Delaware judgment fully resolved the issue of whether SSL infringes Stambler's patents, this

[1] Copies of the patents-in-suit and all other exhibits referenced herein are attached as Exhibits to the Declaration of Jonathan Hardt in Support of JPMorgan's Motion to Dismiss Based on the Preclusive Effect of the Delaware Non-Infringement Judgment, filed contemporaneously herewith ("Hardt Declaration").

case should be dismissed under the doctrine of collateral estoppel and under the doctrine established by the United States Supreme Court in *Kessler v. Eldred*, 206 U.S. 285 (1907).

Statement of Issues

(1) Whether Stambler's claims in this action are barred by the doctrine of collateral estoppel and the judgment of non-infringement as to the SSL protocol in *Stambler v. RSA Security Inc.*, No. Civ. A 01-0065-SLR, 2003 WL 22749855, (D. Del. Nov. 14, 2003) (the "Delaware Action").

(2) Whether Stambler's claims in this action are barred by the *Kessler* doctrine in light of the judgment of non-infringement as to VeriSign, JPMorgan's sole supplier of digital certificates used for secure funds transfer services, in the Delaware Action.

Background

I. The Delaware Action Resolved That SSL 3.0 Does Not Infringe Stambler's Patents

On February 2, 2001, Stambler filed suit against five defendants, including VeriSign and RSA Security, Inc. ("RSA"), alleging infringement of three patents, including the '148 Patent and the '302 Patent—the same two patents Stambler has asserted against the defendants in this case. *Stambler*, 2003 WL 22749855, at *1.[2] At the time, RSA provided several products, including ACE and BSAFE products, "to implement SSL functionality into products and services that perform [] financial transactions." Trial Tr. 126:1-5, Feb. 26, 2003 (Ex. E).[3] VeriSign sold digital certificates and other products that could be used in SSL version 3.0 protocol to verify the identity of participants in secure SSL communications. *See* Trial Tr. 469-475, Feb. 27, 2003 (Ex. F).

The common denominator was SSL version 3.0. In discovery and pretrial proceedings in the Delaware Action, Stambler repeatedly contended that the use of SSL version 3.0 infringed his patents, including the use of SSL to conduct funds transfers over the Internet with banks.

---

[2] A related declaratory judgment action between Stambler and VeriSign (2:08-cv-00348-DF) raised the issue of preclusion. That case settled before the issue was resolved.

[3] Unless otherwise noted, all hearing and trial transcript references are to the Delaware Action, and are attached to the Hardt Declaration as Exhibits C through I.

During claim construction proceedings, Stambler's counsel used Internet banking secured by an SSL session as an alleged example of the claimed invention:[4]

> We'll use for our example an electronic banking transaction and, in particular, one application of the invention is that it's specifically referenced in the patents that of a bill payment system.

See Markman Hr'g Tr. 8:21-25, Jan. 8, 2003 (Ex. B).

When the district court decided to give RSA and VeriSign separate trials on Stambler's claims of infringement against them, Stambler successfully persuaded the court to reconsider that decision.[5] Stambler argued that his case against both defendants would be the same: in essence, that their accused products necessarily resulted in the use of SSL version 3.0, and that the use of SSL version 3.0 was what infringed his patents. *See* Trial Tr. 17:1-25, Feb. 24, 2003 (Ex. D); *Stambler*, No. Civ. A 01-0065-SLR, Dkt. No. 414 (Feb. 21, 2003 Letter to Judge Robinson) at 1, 5 (Ex. J) (explaining that Stambler's patent claims were focused on the SSL protocol—and that "the SSL infringement issues are factually the same for both RSA and VeriSign."). At a pre-trial hearing on the issue, Stambler's counsel summed up his claims clearly:

> ***"It's SSL 3.0. That's what this case is about. And that's what this case will decide."***

Trial Tr. 17:24-25, Feb. 24, 2003 (Ex. D) (emphasis added). Judge Robinson ultimately agreed, reasoning that Stambler "ha[d] represented that the infringement issues in th[e] case are not so much based on each defendant's products but on an industry protocol." *See* Trial Tr. 4:6-9, Feb. 24, 2003 (Ex. D).[6]

---

[4] Stambler was represented by different counsel in the Delaware Action.

[5] During the Delaware Action, RSA and VeriSign moved for separate trials on the grounds that each defendant offered separate products. *See Stambler*, No. Civ. A 01-0065-SLR, Dkt. No. 357 (Jan. 22, 2003 Motion by RSA, Inc. to Sever) (Ex. K). On February 20, 2003, the court granted the motion. *Id.*, Dkt. No. 412 (Feb. 20, 2003 Order Granting Motion to Sever) (Ex. L).

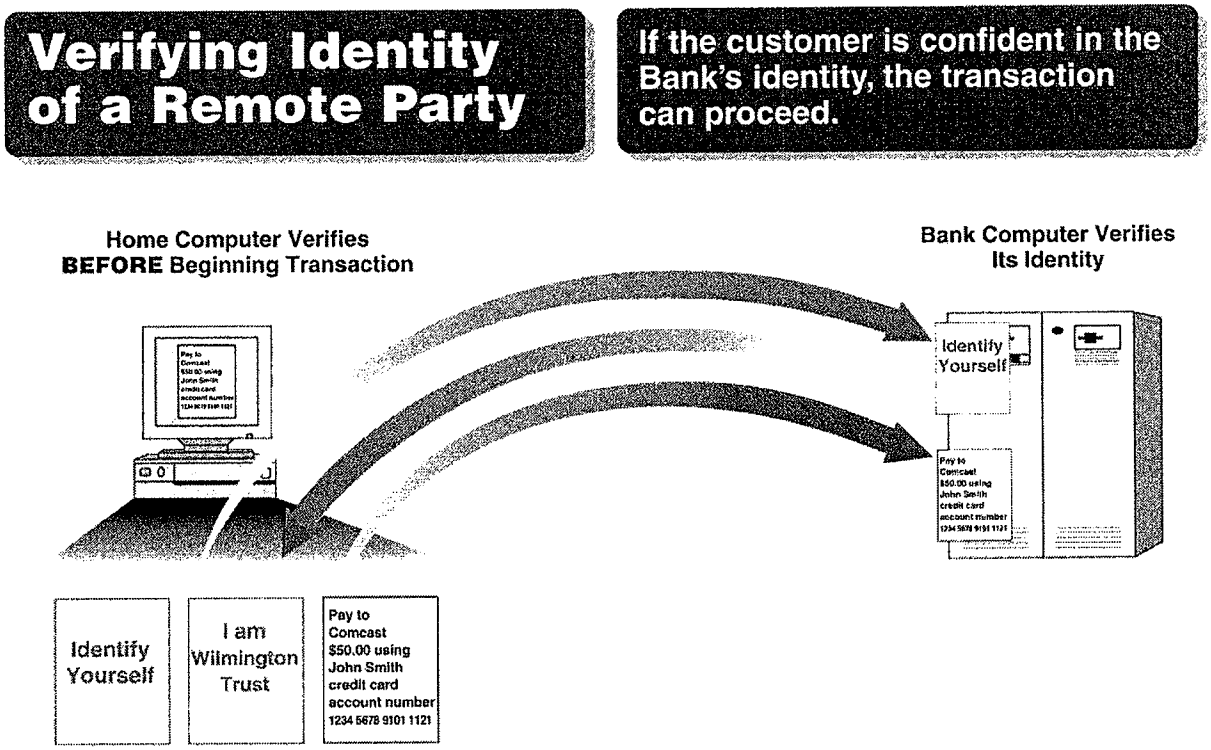
[6] *See also* Trial Tr. 34:4-10, Feb 24, 2003 (Ex. D) (setting out Judge Robinson's conclusion, "All right. I have reviewed the expert reports, and it is clear to me that much of the case is going to be on the SSL protocol. If you look at the expert reports, probably 90 to 95 percent of the reports have to do with the protocol and not with individual products. So I have decided that plaintiff's position is the more correct one.").

A jury trial was held from February 24 through March 7, 2003. The issue at trial was whether the use of SSL version 3.0 by VeriSign and RSA infringed claim 34 of the '302 patent or claims 1, 16, or 35 of the '148 patent. Stambler's expert, Dr. Finkel, testified that in his opinion ***any*** use of the SSL protocol infringed Stambler's patents. *See, e.g.*, Trial Tr. 436:5-9, Feb. 27, 2003 (Ex. F) (setting out his opinion that "the use of SSL Version 3.0 or TLS or WTLS infringes [the patent claims at issue].") Further, he referred to SSL-enabled online banking transactions as examples of allegedly infringing activity. *See, e.g.*, Trial Tr. 423:25-436:9, Feb. 27, 2003 (Ex. F). Dr. Finkel's trial testimony even featured a hypothetical SSL session used in online banking in which "John Smith" uses his home computer to pay his cable bill by providing information via the Internet to his bank. As Dr. Finkel explained:

> So the example is that we have someone sitting at their home computer. It seems to be Mr. John Smith. And he wants to pay his bill and this is his cable bill and so he wants to send a message to his bank to pay 850 to Comcast and it lists his name and his credit card number.
>
> . . . .
>
> And so now we see this message, this message is now being sent to the bank, and when the bank receives it, it will be able to read the message and then it will execute this transaction.

Trial Trans. 357:4-13, Feb. 26, 2003 (Ex. E).

Among the demonstrative exhibits used to illustrate Professor Finkel's "Mr. Smith" hypothetical was the slide reproduced below:



Trial Demonstrative (Ex. N); see also Trial Tr. at 371:6-374:21, Feb. 26, 2003 (Ex. E). Among other things, this slide discusses the concept of using SSL version 3.0 and digital certificates to verify the identity of the bank computer to its online banking customer. As Dr. Finkel concluded: "the use of SSL Version 3.0, TLS, or WTLS, infringes Claim 34 of the '302 patent, and when they are used for certain financial transactions, they would infringe Claims 1, 16 and 35 of the '148 patent." *See* Trial Tr. 436:5-9, Feb. 27, 2003 (Ex. F).

Stambler's counsel also argued repeatedly to the jury that the issue they had to decide was whether SSL 3.0 infringed Stambler's patents. During opening statements to the jury, Stambler's counsel framed the issue thus:

> You are going to hear in this case about one particular security method, a method that is used to secure information in products sold by VeriSign and RSA that we say infringe Mr. Stambler's patents, and that's a method called SSL, which is short for secure sockets layer.

Trial Tr. 169:3-8, Feb. 26, 2003 (Ex. E). And in closing, Stambler's counsel further argued to the jury:

> [Y]ou have to compare the claims to SSL as they're used in the products. And when you do that, you see that every element of the claims is met. The claims are infringed.

See Trial Tr. 1448:23-1449:1, Mar. 6, 2003 (Ex. I). Stambler's counsel summarized his claim as follows:

> We talked about a number of specific claims in Mr. Stambler's patents that are infringed by the use of SSL Version 3.
>
> Now, defendants sell products which use SSL Version 3 or TLS. They don't have permission from Mr. Stambler to use his patents which cover those protocols and that means that they're infringing his patents, and that's wrong.
>
> Now, you're going to hear from Judge Robinson in this case that the infringement analysis, what that involves is taking the claims, the number of paragraphs we've been looking at, and comparing that to what happens in SSL as used by the defendants' products. That's what an infringement analysis is. It's a comparison of the claims with the SSL protocol specification. That's the issue here. There is no doubt about it.

Trial Tr. 1348:13-1349:4, Mar. 6, 2003 (Ex. I).

The jury returned a verdict of non-infringement of all claims in favor of VeriSign and RSA. *See Stambler*, 2003 WL 22749855, at *1. Following judgment, Stambler moved for a directed verdict, in part, based on the contention that "under the court's claim construction and on the basis of the expert testimony from both sides, all the limitations of claim 34 are present and no reasonable jury could conclude otherwise." *Stambler*, 2003 WL 22749855, at *4. In denying Stambler's motion, the court characterized the infringement issue solely in terms of SSL version 3.0: "In order for plaintiff to prove that defendants induced infringement, plaintiff must show that SSL 3.0 literally infringes claim 34. ***The jury concluded that SSL 3.0 did not literally infringe claim 34 of the '302 patent.***" *Id.* at *4 (emphasis added).

The finding of non-infringement—and subsequent judgments—were affirmed by the Federal Circuit on appeal. *Stambler v. RSA Security, Inc.*, Nos. 04-1129, 04-1147, 04-1148, 2005 WL 352606, at *1 (Fed. Cir. Feb. 11, 2005). As the Federal Circuit noted:

> Stambler sued RSA for, inter alia, infringement of the '302 patent based on its use of Secure Sockets Layer version 3.0 ("SSL 3.0"). The patented methods enable parties to a transaction to assure the identity of an absent party and the accuracy of information involved in the transaction, thus providing for secure transactions and preventing fraud. SSL 3.0 is widely considered to be the standard method for conducting secured communications via the Internet.

Id. (internal citations omitted). Agreeing that substantial evidence demonstrated that the use of SSL version 3.0 did not infringe, the Federal Circuit affirmed the jury's verdict and the district court's judgment. *See id.* at *3.

II. The Delaware Action Also Resolved That VeriSign's Digital Certificates, When Used As A Credential, Do Not Infringe Stambler's Patents

In the Delaware Action, Stambler contended that VeriSign's sale of digital certificates for use in the SSL version 3.0 protocol infringed his patents. For example, Stambler's counsel explained to the Delaware court the importance of credentials to verify the identity of parties to an SSL session as follows:

> [I]t turns out that there are electronic forms of credentials called digital certificates. . . . VeriSign, who is in the business of issuing digital certificates, they are the most robust form of credential in the digital world.
>
> A digital certificate is basically a data file that can be stored on computer and sent to another computer when the need to prove one's self arises.
>
> If we take a look at the format of a typical digital certificate on the left, well, it contains a lot of things that computers need to know in order to talk to each other, like versions and identification of the algorithms they're going to use and so on. But for our purposes, what's important is, number one, the certificate contains information about who the certificate was issued to, which is called the subject.
>
> The certificate also contains a cryptographic key that's associated with the subject and that's important. We'll talk about how that's used in a moment.
>
> Finally, the certificate contains something called a signature of the authority that issued the certificate, which is a digital code that proves that the trusted authority and no one else could have sent or generated that certificate.

Markman Tr. 18:14-19:17, Jan. 8, 2003 (Ex. C).

As described above, the jury rejected Stambler's claim in the Delaware Action, and the judgment of noninfringement was affirmed on appeal. Nonetheless, nearly four years later, Stambler has made allegations in this case that are identical to the ones rejected in Delaware.

III. Stambler's Claims In This Action Are Barred by the Delaware Judgment of Non-Infringement.

On May 12, 2008, Stambler filed his initial complaint in the present action [Dkt. No. 1] alleging that 29 defendants, which generally engage in online banking services, infringe the '302 patent. On August 15, 2008, Stambler filed an Amended Complaint [Dkt. No. 154], alleging that 28 of the original defendants, plus an additional defendant, also infringe the '148 patent. Both patents were asserted in the Delaware Action; indeed, several of the claims originally asserted in this proceeding were previously asserted in Delaware. *Compare* Stambler's '148 Patent Infringement Contentions (including the assertion of claims 1, 16, 28 and 35 of the '148 Patent in this case) (Ex. P) *with* Plaintiff's Supplemental Responses to Defendants' Joint Interrogatory Nos. 1, 5, 7, 12, and 13 in the Delaware Action at 2-19 (asserting claims 1, 16, 28 and 35 of the '148 patent in the Delaware Action) (Ex. M); *and* Stambler's '302 Patent Infringement Contentions (including the assertion of claim 34 of the '302 Patent) (Ex. Q) *with* Plaintiff's Supplemental Responses to Defendants' Joint Interrogatory Nos. 1, 5, 7, 12 and 13 in the Delaware Action at 2-19 (Ex. M) (setting out in the Delaware Action, *inter alia*, infringement allegations involving claims claim 34 of the '302 Patent). After Stambler narrowed his claims on July 27, 2009 [Dkt. No. 316], pursuant to the Court's order, claim 35 of the '148 patent is still asserted, despite the fact that Stambler specifically asserted, and lost, on that claim in Delaware. Just as importantly, the Stambler Infringement Contentions relating to all other asserted claims in this case involve the SSL version 3.0 protocol, and each necessarily involves VeriSign Digital

Certificates. JPMorgan only uses VeriSign digital certificates for secure funds transfer services. *See* JPMorgan's Supplemental Responses to Plaintiff's First Set of Interrogatories, at 8 (Ex. O).

As noted above, in this action Stambler asserts claims 28, 34, and 35 of the '148 patent. *See* Stambler's '148 Patent Infringement Contentions at 21-32 (Ex. P). Each and every one of the claims that Stambler asserts involves "creating a variable authentication number (VAN)."[7] Stambler contends that "a VAN is created by generating . . . a keyed MAC using at least a portion of the information for identifying the payee and the amount and the client write MAC secret, which is derived from the master secret." *See, e.g.*, Stambler's '148 Patent Infringement Contentions at 22 (setting forth Stambler's accusations surrounding claim 28).[8] In JPMorgan's accused systems, the information that Stambler alleges to be "keyed MACs" and/or "VANs" is derived exclusively by using VeriSign Digital Certificates in the SSL version 3.0 protocol—the same VeriSign Digital Certificates and the same SSL version 3.0 protocol that were determined not to infringe in the Delaware Action.

Likewise, the asserted claims from Stambler's '302 patent all involve either creating a "VAN" for authentication, or authenticating information with a "credential."[9] In any event, the VeriSign Digital Certificates and the SSL version 3.0 protocol are at the heart of every claim. The alleged "VAN" is derived by using the VeriSign Digital Certificate in the SSL version 3.0 protocol, and Stambler has alleged in this action (as he alleged in Delaware) that the VeriSign

---

[7] *See, e.g.*, '148 Patent claim 1, 16 (Ex. A); *see also id.* claim 34 (using slightly different wording, "using a computer to create a variable authentication number (VAN)"); *id.* claim 35 ("creating the VAN").

[8] *See also* Stambler's '148 Patent Infringement Contentions at 28 (Ex. P) (using slightly different language with regard to claim 34: "creates a VAN by generating . . . a keyed MAC using the funds transfer information and the client write MAC secret, which is derived from the master secret."); Stambler's '148 Patent Infringement Contentions at 32 (Ex. P) (asserting for claim 35: "creates a VAN by hashing the EDC1 and the client write MAC secret").

[9] *See* '302 Patent, claim 41, 43, 46, 47, 48 (dependent on claim 41) (Ex. B) ("generating a [VAN] at least a portion of the received funds transfer information"); *id.* claim 53 (dependent on claim 51, which is "[a] method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party . . . ."). Stambler has withdrawn Claim 51 of the '302 Patent, but has continued to assert claims 52 through 55, dependent on Claim 51; his infringement contentions with respect to Claim 51 are, therefore, still relevant.

Digital Certificate is the "credential." *See, e.g.,* Stambler's '302 Patent Infringement Contentions at 2 (Ex. Q) ("Prior to the transaction, a digital certificate (i.e. the credential) was issued to Defendant by a trusted party (i.e. a certificate authority).").

Argument

In this action, Stambler accuses the same process (SSL 3.0) and the same instrumentalities (VeriSign Digital Certificates, and the information generated from those certificates when used in SSL) of infringing the same patents that he litigated unsuccessfully in the Delaware Action. *See, e.g.*, Trial Tr. 436:25-437:1, Feb. 27, 2003 (Ex. F) ("So part of the SSL protocol is to authenticate a party using a digital certificate"). He is precluded from doing so by at least two well established doctrines: the doctrine of collateral estoppel and the *Kessler* doctrine.

I. Collateral Estoppel Precludes Stambler From Pursuing the Same Theory of Infringement Against JPMorgan as He Did in the Delaware Suit

Stambler is precluded from pursuing this suit under fundamental principles of collateral estoppel—he has already litigated, and lost, the same issue presented in this case. In both cases, the products are the same with respect to every aspect relevant to his claims. Thus, Stambler effectively is attempting to re-litigate factual issues that were previously resolved, which the doctrine of collateral estoppel clearly precludes.

A. Collateral Estoppel Precludes a Nonmoving Party from Vexatiously Multiplying Litigation, and Taxing Judicial Resources Simply by Switching Adversaries and Relitigating the Same Issue

As the Federal Circuit has held, "[c]ollateral estoppel precludes a plaintiff from relitigating identical issues by merely switching adversaries and precludes a plaintiff from asserting a claim that the plaintiff had previously litigated and lost against another defendant." *A.B. Dick Co. v. Burroughs Corp.*, 713 F.2d 700, 702 (Fed. Cir. 1983) (internal citations omitted)

(emphasis added); *see also In re Freeman*, 30 F.3d 1459, 1465 (Fed. Cir. 1994) (under the doctrine of collateral estoppel, a judgment on the "merits in a first suit precludes relitigation in a second suit of issues actually litigated and determined in the first suit."). The doctrine protects parties against multiple unnecessary litigations, and prevents inconsistent decisions while preserving judicial resources for issues that have not already been adjudicated. *See In re Freeman*, 30 F.3d at 1465 ("a party who has litigated an issue and lost should be bound by that decision and cannot demand that the issue be decided over again."); *U.S. v. Shanbaum*, 10 F.3d 305, 311 (5th Cir. 1994) (collateral estoppel "promotes the interests of judicial economy"); *MGA, Inc. v. General Motors Corp.*, 827 F.2d 729 (Fed. Cir. 1987) (collateral estoppel "relieve[s] parties of the cost and vexation of multiple lawsuits, conserve[s] judicial resources, and, by preventing inconsistent decisions, encourage[s] reliance on adjudication."). In particular, "defensive collateral estoppel gives a plaintiff a strong incentive to join all potential defendants in the first action." *Parklane Hosiery Co., Inc. v. Shore*, 439 U.S. 322, 329-330 (1979).

Vexatious multiplicity of litigation, which burdens defendants and consumes judicial resources, is precisely what collateral estoppel is designed to prevent. *See In re Freeman*, 30 F.3d 1459 (applying collateral estoppel to preclude patentee from relitigating the scope of a claim term during reexamination); *Molinaro v. Fannon/Courier Corp.*, 745 F.2d 651 (Fed. Cir. 1984) (per curiam) (determination of noninfringement in prior action alleging infringement of the same patent by similar receivers was entitled to collateral estoppel effect, where issues of infringement were identical to those previously decided); *Studiengesellschaft Kohle, mbH v. USX Corp.*, 675 F. Supp. 182, 182 (D. Del. 1987) (plaintiff was collaterally estopped from claiming infringement by a certain chemical process, where it had unsuccessfully claimed the same in a prior litigation against different defendant; in both cases, plaintiff asserted the same rationale for

infringement, and "simply name[d] a different party . . . ."); *Molinaro v. Sears, Roebuck and Co.*, 478 F. Supp. 818 (D.C.N.Y. 1979) (finding summary judgment on noninfringement appropriate where collateral estoppel barred plaintiff from pursuing its theory of infringement that patent covered certain radio receivers, where similar receivers had been found not to infringe plaintiff's patent under same theory in multiple previous litigations). The Supreme Court has clearly noted that "repeated litigation of the same issue as long as the supply of unrelated defendants holds out reflects either the aura of the gaming table or a lack of discipline and of disinterestedness on the part of the lower courts, hardly a worthy or wise basis for fashioning rules of procedure." *Blonder-Tongue Labs, Inc. v. Univ. of Illinois Found.*, 402 U.S. 313, 329 (1971).

Collateral estoppel is particularly appropriate in the patent infringement context where needless multiplication of litigation hinders the ability of producers and sellers to market their products. *Studiengesellschaft*, 675 F. Supp. at 188 ("***The exigencies of litigation demand that at some point there be an end to litigation of a particular issue. This is particularly so in the context of patent litigation.*** Relitigation of infringement issues already decided not only forces producers and sellers of products to divert their resources away from productive uses in favor of repetitious litigation but also hampers their ability to effectively and efficiently produce and market their products.") (emphasis added); *see also Parklane Hosiery,* 439 U.S. at 329 n.10 ("relitigation of issues previously adjudicated is particularly wasteful in patent cases because of their staggering expense and typical length.").

B. Collateral Estoppel Applies Here Because Whether SSL Version 3.0 Infringes Stambler's Patents Has Already Been Definitively Adjudicated In The Delaware Suit

Under the Federal Circuit's test, to prevail on the theory of collateral estoppel, a party must show the following: "(1) the issue is identical to one decided in the first action; (2) the issue was actually litigated in the first action; (3) resolution of the issue was essential to a final

judgment in the first action; and (4) plaintiff had a full and fair opportunity to litigate the issue in the first action." *In re Freeman*, 30 F.3d at 1465; *see also U.S. v. Shanbaum*, 10 F.3d 305, 311 (5th Cir. 1994) (setting forth a similar test). Each element of the test is satisfied here.

1. The Issues Here and in Delaware Are Identical

As set forth above, every one of Stambler's infringement contentions in this case contains the allegation that SSL version 3.0, when used to facilitate funds transfer, satisfies the limitations of Stambler's asserted patent claims. Thus, the allegation that SSL version 3.0 infringes the asserted patents pervades all of Stambler's infringement contentions in this case. That issue is identical to the issue actually litigated and decided in the Delaware Action.

Stambler has argued that this case involves questions not exactly identical to those decided in the Delaware Action. He asserts that the accused products and services—online banking and funds transfer—are different from what was accused in Delaware. *See* Plaintiff's Opposition to Defendant's Motion to Stay Pending Outcome of a Related Declaratory Judgment Action (Dkt. No. 259) (hereinafter "Opposition to Motion to Stay") at 2-3.[10] As shown above, however, a careful inspection of the record in the Delaware Action proves otherwise.

More particularly, in the Delaware Action, Stambler repeatedly alleged before and during trial that ***any*** use of SSL version 3.0 infringed his patents, including its use in online banking and funds transfers. *See* Background Section I, *supra*; Markman Hr'g Tr. 7:2-23:12, Jan. 8, 2003 (Ex. C); Trial Tr. 355:9-357:8, Feb. 26, 2003 (Ex. E); Trial Tr. 423:25-431:7, 436:5-9, Feb. 27, 2003 (Ex. F). Thus, the Delaware Action and resulting judgment necessarily settled the identical

[10] As the Court will recall, Defendants filed their Motion to Stay Pending the Outcome of a Related Declaratory Judgment Action on November 14, 2008 [Dkt. No. 236], seeking to have this case stayed while the Court determined the issues raised in the present motion—issues that were then the crux of a related, and recently filed, declaratory judgment action between Stambler and VeriSign. *See* Dkt. No. 236 at 1-2. That action has since been dismissed. *See Stambler v. VeriSign, Inc.*, No. 2:08-cv-00348-DF [Dkt. No. 32].

question presented here—whether SSL version 3.0 infringes Stambler's patents. The answer to that question, as fully adjudicated in the Delaware Action, is no.

Stambler also has asserted that "in the patent infringement context, issues are not identical where, as here, the accused instrumentalities in the first and second suits are different." *See* Opposition to Motion to Stay at 14. That argument is incorrect as a matter of law. *Studiengesellschaft*, 675 F. Supp. at 188. In that case, the court noted, in words equally applicable here, that "[plaintiff] next argues that because infringement claims necessarily involve consideration of a specific accused product or process, collateral estoppel can never be based on a prior judicial finding that another defendant's product or process does not infringe a patent. ***Under [plaintiff's] analysis, no prior infringement decision could ever serve as the basis for collateral estoppel unless it involved the same defendant and the same product as are involved in the second action. Federal Circuit precedent is plainly to the contrary.***" *Id.* (emphasis added) (citing *Molinaro v. Fannon/Courier Corp.*, 745 F.2d 651 (Fed. Cir. 1984) (per curiam)).

In any event, Stambler has expressly asserted that the use of SSL version 3.0 is central to the accused instrumentalities in this case.[11] Both the accused instrumentalities and his theory of infringement here and in the Delaware Action are identical: SSL version 3.0 allegedly infringes his asserted patents.

[11] *See, e.g.*, Stambler's '148 Patent Infringement Contentions Claim 28 at 23-24 (Ex. P) ("[T]he customer's computer creates an encrypted SSL and/or TLS record layer message that includes the information for identifying the Defendant and the amount, and the VAN, and sends it to the Defendant's server. The SSL and/or TLS record layer message is an instrument that is used to pay the credit card debt."); *id.* Claim 34 at 28 ("When Defendant and its customer communicate using SSL and/or TLS, the Defendant's server and the customer's computer complete a 'handshake' process that results in the generation of a 'master secret,' which is used to generate other keys and secrets."); *id.* Claim 35 at 31 ("The first party sends the information regarding the requested funds transfer (and, as described below, the VAN) to a second computer in an encrypted SSL and/or TLS record layer message (i.e. the instrument)."); Stambler's '302 Patent Infringement Contentions Claim 7 at 1 (Ex. Q) ("Defendant offers secure online bill payment services and secure online funds transfer using Secure Sockets Layer protocol ("SSL") and/or Transport Layer Security protocol ('TLS')."); *id.* Claim 41 at 14 ("When Defendant and its customer communicate using SSL and/or TLS, the Defendant's server and the customer's computer complete a handshake process that results in the generation of a 'master secret,' which is used to generate other keys and secrets."); *id.* Claim 53 (Dependant on Claim 51) at 28 ("The second party's server decrypts the received SSL and/or TLS record layer message.").

2. Whether SSL Infringed the Asserted Patents Was Essential to the Final Judgment in Delaware

The second element of the collateral estoppel test—whether "resolution of the issue was essential to a final judgment in the first action"—is also met here. *In re Freeman*, 30 F.3d at 1465. In his opposition to the motion to stay, Stambler suggests that this element is not satisfied because the Delaware court allegedly did not specify whether final judgment was based on Stambler's "failure to demonstrated intent to induce infringement by VeriSign or the lack of direct infringement by the induced party." Stambler Opposition at 14. This is not true.

As an initial matter, Stambler brought a claim for direct infringement in Delaware and lost. Contrary to Stambler's assertions, he did not "voluntarily withdr[a]w" direct infringement from the previous case "for tactical reasons." Stambler's Surreply in Opposition to Motion to Stay [Dkt. No. 283] at 7. In fact, the district court granted defendant's motion for judgment as a matter of law for no direct infringement. *See* Trial Tr. 1012:23-24, Mar. 3, 2003 (Ex. H) ("We moved that there is no proof of direct infringement by VeriSign."); Trial Tr. 1321:5-9, Mar. 6, 2003 (Ex. I) (Stambler's counsel reserving the right to argue that sufficient evidence on the record to support direct infringement); *see generally* Trial Tr. 1012:23-1013:19, 1017:23-1018:16, Mar. 3, 2003 (Ex. H).

Although a *claim* for direct infringement was not presented to the jury (because it was subject to JMOL, not because Stambler voluntarily withdrew it), the *issue* of direct infringement was squarely before the jury and essential to the final judgment.

Both the district court and the Federal Circuit held that substantial evidence supported the conclusion that SSL does not infringe the asserted patents and affirmed the Delaware jury's verdict on that basis. *Stambler*, 2003 WL 22749855, at *2-6; *RSA Security, Inc.*, 2005 WL 352606, at *1 (Fed. Cir. 2005). The district court's opinion explicitly found that substantial

evidence supported the jury's finding that the SSL version 3.0 did not directly infringe Stambler's patents:

> Having concluded that there was substantial evidence whereby a reasonable jury could conclude that SSL 3.0 does not infringe any of the three contested limitations of claim 34 of the '302 patent, the court will deny plaintiff's motion for judgment as a matter of law.

Stambler, 2003 WL 22749855 at *6; *see also id.* at *4 ("The court finds that a reasonable jury could have concluded that the digital certificate is not a credential within the meaning of claim 34 . . . ."); *id.* at *5-6 (finding that the jury reasonably could have concluded that the other two disputed limitations were not present in SSL version 3.0). Likewise, the Federal Circuit specifically affirmed this finding: "[b]ecause ***substantial evidence supports the finding that SSL 3.0 does not contain a "credential" as construed by the district court***, we need not discuss the other disputed limitations, as a product must contain each and every limitation of a claim in order to infringe that claim." *RSA Security, Inc.*, 2005 WL 352606, at *3 n.2 (emphasis added); *see also id.* at *2-3 ("RSA's expert simply took the district court's claim construction and provided detailed testimony as to why the accused device did not meet the claim limitations. . . . Based on the record, including the testimony of RSA's expert, we conclude that substantial evidence supports the jury's verdict of non-infringement.").

A finding of infringement now necessarily would be inconsistent with the finding of non-infringement in Delaware. As in Delaware, Stambler's infringement contentions expressly accuse SSL version 3.0. *See, e.g.*, Stambler's '148 Patent Infringement Contentions at 1 (Ex. P). Stambler's infringement contentions for every element of every claim at issue in this litigation are the same as the contentions asserted and tried in Delaware. While a chart outlining each infringement contention here and the corresponding trial testimony in Delaware is attached as

Exhibit S to the Hardt Declaration, a look at even one example makes the overlap between the Delaware Action and this case abundantly clear:

<table>
<tr><th colspan="2">Claim 35 Element</th></tr>
<tr><td colspan="2">an originator party creating an instrument for transferring funds to a recipient party, the instrument information comprising (i) a variable authentication number (VAN), and (ii) one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number;</td></tr>
<tr><th>Stambler's Current Infringement Contention</th><th>Matching Delaware Testimony</th></tr>
<tr><td>Defendant's customer creates an instrument for transferring funds to the recipient of the bill payment. When Defendant's customer logs onto the Defendant's website and chooses to transfer funds to a second party using Defendant's online webpage through which the customer enters on or more pieces of payment information, including information for identifying the customer, information for identifying the recipient, the amount of the bill payment, and/or a date.
'148 Infringement Contentions at 30.</td><td>Q. Claim 35. Can you walk us through this one? This has a few little additional elements maybe you could explain for us.
A. Okay. So again we have, this is a funds transfer method, so we're still thinking about a refund payment from a merchant to a customer and the merchant is using [VeriSign's product]. And now we have, the two parties here are described as an originator party and the recipient party. So the originator party is the merchant and the recipient party is the customer. And the originator party creates an instrument for transferring funds, so that's going to be the SSL message that it sends, the merchant sends to the [VeriSign product] server.
Q. Okay. Now, next the claim provides that the instrument information comprises two things, a variable authentication number and one or more pieces of payment information, including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number.
Do you see that?
A. Yes.
. . . .
Q. But could you tell us how the instrument that you referred to that is made in [VeriSign's product] meets this limitation of the claim?
A. Yes. I'm sorry. The instrument, as I said, is the SSL message with the payment information and the message authentication code and so that's the variable authentication number is the message authentication code. And the message also contains, it says here, one or more pieces of information. In our case, we have several pieces of payment information. We have the amount. We have information for identifying the recipient party, and we also have information for identifying the originator party. So that would be the customer and the merchant.
Trial Tr. 487:23–489:9, Feb. 27, 2003.</td></tr>
</table>

In short, whether SSL version 3.0 infringes the asserted patents was vigorously litigated at trial and resolved by a jury. It was then an issue addressed by the district court and the Federal Circuit, ***at Stambler's prompting***, after which both courts sustained the jury's finding of noninfringement. In other words, it was an issue essential to the judgment against Stambler. In instances such as these, collateral estoppel is appropriate. *In re Freeman*, 30 F.3d at 1465 ("Where an appellate court has decided a specific question, the doctrine of issue preclusion should normally prevent relitigation of that issue."); *Molinaro*, 745 F.2d at 655 ("where a determination of the scope of patent claims was made in a prior case, and the determination was essential to the judgment there on the issue of infringement, there is collateral estoppel in a later case on the scope of such claims"); *Studiengesellschaft*, 675 F. Supp. at 184 (appeals court's holding in prior case made clear that noninfringement was based precisely on the fact that patent did not cover claimed process); *see also Mother's Rest., Inc. v. Mama's Pizza, Inc.*, 723 F.2d 1566, 1571 (Fed. Cir. 1983) (noting the relatively low standard to satisfy this element of the collateral estoppel test—which the instant case more than satisfies: "it is important to note that the requirement that a finding be 'necessary' to a judgment does not mean that the finding must be so crucial that, without it, the judgment could not stand. Rather, the purpose of the requirement is to prevent the incidental or collateral determination of a nonessential issue from precluding reconsideration of that issue in later litigation.").

3. Whether SSL Infringes the Asserted Patents Was Actually Litigated in the Delaware Suit

This aspect of the collateral estoppel test is not in dispute. Stambler raises no objection on this basis in the collateral estoppel section of his opposition to the motion to stay. Stambler Opposition at 14-15. It would strain credulity to suggest otherwise.

4. Stambler Had a Full and Fair Opportunity to Litigate the Issue in the Delaware Action

Similarly, that Stambler had a full and fair opportunity to litigate this issue cannot reasonably be disputed. In Delaware, Stambler asserted both patents at issue here and (originally) seven claims resulting in a four years of litigation, culminating in a seven-day jury trial, post-trial briefings, and a Federal Circuit appeal. Throughout that time, whether SSL infringed the asserted patents was at the forefront.

Thus, the previous lawsuit provided a more than full and fair opportunity to litigate the issue. *See, e.g.*, *In re Freeman*, 30 F.3d at 1467 ("the fact that this court on appeal affirmed the district court's conclusions regarding . . . noninfringement strongly suggests that the district court proceedings were not deficient"); *Studiengesellschaft*, 675 F. Supp. at 186-87 (rejecting nonmovant's assertion that the court's application of prevailing law in previous lawsuit was deficient: "[nonmovant's] argument amounts to nothing more than a collateral attack on the correctness of the appellate court's decision. It has long been clear, however, that in deciding whether collateral estoppel is appropriate in a particular case, it is improper to inquire whether the prior judgment is correct."). Accordingly, the elements for application of collateral estoppel are all present here and this Court should accordingly dismiss Stambler's infringement claims.

II. The *Kessler* Doctrine Precludes Needless Multiplicity Of Lawsuits Where, Like Here, A Patentee Has Previously Lost On The Same Claims

While the *Kessler* doctrine is fundamentally similar to the collateral estoppel doctrine, it clearly developed as an instrument to safeguard the purchase and use of products that have been previously found not to infringe the patents of another. *See Rubber Tire Wheel Co. v. Goodyear Tire & Rubber Co.*, 232 U.S. 413, 417-18 (1914) (noting that *Kessler* creates a trade right that "include[s] the right to have others secure in buying that article, and in its use and resale"). As the Federal Circuit has made clear, "[t]he *Kessler* doctrine bars a patent infringement action

against a customer of a seller who has previously prevailed against the patentee because of invalidity or noninfringement of the patent; otherwise, the effect of the prior judgment would be virtually destroyed." *See MGA, Inc. v. General Motors Corp.*, 827 F.2d 729, 734 (Fed. Cir. 1987).

In *Kessler*, Eldred, the owner of a patent for an "electric lamp lighter" sued his competitor (Kessler) for infringement. *See Kessler v. Eldred*, 206 U.S. 285, 285 (1907). The district court found that Kessler's lighter did not infringe, and the Seventh Circuit affirmed. *See id.* at 285-86. Four years later, Eldred sued Breitweiser, a Kessler customer, for infringement; Kessler then filed suit to enjoin Eldred from prosecuting infringement claims for the purchase, use, or sale of Kessler's lighters that had been adjudged not to infringe in the original suit between Eldred and Kessler. *See id.* at 286. The Supreme Court held that the lower court could enjoin Eldred from interfering with Kessler's right to manufacture and sell the lighters without threat of Eldred's patent rights.[12] *See id.* at 289. The common thread in both of *Kessler* and its progeny is that the doctrine precludes a plurality of lawsuits where, as here, a Court already has entered a final adverse judgment against a patentee in a lawsuit against the manufacturer involving the same product. *Cf. Unitronics Ltd. v. Gharb*, 532 F.Supp.2d 25, 27-28 (D.D.C. 2008).

A. This Action Constitutes Needless Multiplicity Because The Facts Here Parallel The Circumstances Where *Kessler* Has Been Applied In The Past

In this action, Stambler alleges that JPMorgan's online banking website, Chase Online—which uses digital certificates that are, in all relevant aspects, the same as the ones at issue during the trial in Delaware—infringes the same patents he asserted in Delaware. Stambler's

[12] Courts have allowed customers as well as manufacturers to seek relief under the *Kessler* doctrine. *See General Chem. Co. v. Standard Wholesale Phosphate & Acid Works, Inc.*, 101 F.2d 178, 181 (4th Cir. 1939) ("To hold that [the patentee] is bound by the judgment in suits against other parties with respect to the same subject matter, does him no injustice and prevents unseemly conflict of decision and useless prolonging of a controversy which has been decided against him by the court.").

allegations against JPMorgan's use of SSL version 3.0 in this case are the same as the ones he made against VeriSign in the Delaware Action because the SSL transactions at issue are enabled by the same product—VeriSign Digital Certificates. Furthermore, these facts are similar to facts where courts have found the *Kessler* doctrine applicable.

For example, in *Unitronics,* a declaratory judgment action brought by Unitronics, the court entered a finding of non-infringement in favor of Unitronics. *Id.* at 27. The *Unitronics* court then enjoined Gharb from pursuing infringement claims against Unitronics' customers and downstream suppliers. *See id.* at 28. The court explained that following its judgment, Gharb's appropriate course of action was to appeal to the Federal Circuit, not the pursuit of other users and buyers of Unitronics' products. An even stronger case under *Kessler* exists in Stambler's suit here, because the Federal Circuit has already upheld the finding of non-infringement in the Delaware Action. *See RSA Security, Inc.*, 2005 WL 352606, at *1.

Stambler's allegations that the online banking systems in this case include new features which are part of his infringement contentions and were not considered during the Delaware Action misses the point. *See* Plaintiff's Opposition to Motion to Stay at 10. Those "new features," such as e-bills, do not speak to the SSL protocol central to Stambler's claims, or the use of VeriSign Digital Certificates. Put simply, to prove that JPMorgan's accused systems infringe, Stambler must show that SSL version 3.0, using VeriSign Digital Certificates, satisfies the same claim elements in his patents that the Delaware court already considered and decided were not infringed.

B. Stambler Is Re-Litigating The Same Claims Against The Same Product

Every one of Stambler's infringement contentions in this case accuses the use of SSL version 3.0 with online banking as the patented funds transfer method.[13] The Delaware Action decided definitively that practicing the SSL version 3.0 protocol for funds transfer while using VeriSign Digital Certificates does not infringe Stambler's patents. *See Stambler*, 2003 WL 22749855, at *1; *RSA Security, Inc.*, 2005 WL 352606, at *1. This case involves the same aspect (SSL version 3.0) of the same instrumentality (online banking using SSL version 3.0) as the Delaware Action. *See, e.g.*, Stambler's '302 Patent Infringement Contentions at 1 (Ex. Q).

Likewise, VeriSign Digital Certificates are the centerpiece of Stambler's claims in both litigations. Stambler continues to assert patent claims in this action that expressly include a credential (digital certificate) as a claim element. *See* Stambler's '302 Patent Infringement Contentions at 1, 22, 24, 32 (Ex. Q) (accusing '302 Patent claims 7, 47, and 53, all of which recite the use of a "previously issued" credential). Further, Stambler contended in Delaware, as he does here, that SSL sessions cannot proceed without the generation of a VAN—a limitation that is met, if at all, through the use of VeriSign Digital Certificates. *See* Markman Hr'g Tr. 213:18-214:2, Jan. 8, 2003 (Ex. C) (counsel arguing, "[t]he simple fact, your Honor, is that Mr. Stambler's patents do disclose the fundamental concepts and ideas that are utilized in the SSL protocol and that's why we're here. Perhaps they don't always use the same language. They say credential rather than certificate or variable authentication number instead of digital signature or message authentication code. But, as Dr. [K]onheim observed, the concepts are disclosed and

[13] *See* Stambler's '148 Patent Infringement Contentions Claim 28 at 21 (Ex. P) ("Defendant offers secure online bill payment services using SSL and/or TLS."); *id.* Claim 34 at 25 ("Defendant offers secure online bill payment using SSL and/or TLS."); *id.* Claim 35 at 29 ("Defendant offers secure online bill payment using SSL and/or TLS."); *see also* Stambler's '302 Patent Infringement Contentions Claim 7 at 1 (Ex. Q) ("Defendant offers secure online bill payment services and secure online funds transfer using Secure Sockets Layer protocol ("SSL") and/or Transport Layer Security protocol ('TLS')."); *id.* Claim 41 at 12 ("Defendant offers secure online bill payment services using SSL and/or TLS."); *id.* Claim 51 at 24 ("Defendant offers secure online bill payment services using SSL and/or TLS.").

described in a way that's recognizable to those who are working in computer science."). JPMorgan does not use any digital certificates in the accused services other than those supplied by VeriSign. JPMorgan's secure implementation of SSL for funds transfer cannot possibly create or generate an accused VAN without operating in the same way as the system that was accused, and found not to infringe, in the Delaware Action.

Finally, Stambler cannot, as he purports to do, avoid the effect of the prior judgment by pretending to carve digital certificates out from this case. *See* June 8, 2009 Bumgardner Letter re: *Leon Stambler v. JP Morgan Chase & Co., et al.* at 1 (Ex. R) (attempting to carve out certain claims "to the extent Plaintiff's infringement contentions specify an accused instrumentality that involves a VeriSign digital certificate"). Digital certificates are central to implementation of the SSL version 3.0 protocol. They are always used to generate the session keys that are used to generate a MAC (which Stambler accuses as the "VAN" of the patent claims), and are always required to begin a session of the accused SSL protocol on JPMorgan's accused funds transfer website. *See, e.g.*, Trial Tr. 665:21-665:15, Feb. 28, 2003 (Ex. G) (Stambler's expert explaining the use of digital certificates in SSL version 3.0 and testifying that "[t]hese web servers rely on the server side certificate to identify themselves to the web browser. And the web browser relies on the certificate to make sure that the server is who they say they are")

C. VeriSign's Digital Certificates Have Not Changed

Stambler previously argued that the *Kessler* doctrine is not applicable here because the VeriSign Digital Certificates used today are in some unspecified way supposedly different from the digital certificates at issue in the Delaware Action. *See* Opposition to Motion to Stay at 11-12. But there is no functional distinction between the VeriSign Digital Certificates used today and the ones in use at the time of the Delaware Action. The VeriSign Digital Certificates

currently used by JPMorgan in an SSL version 3.0 transaction, like the ones accused in the Delaware Action, are used to verify the identity of the certificate holder (when used in conjunction with the certificate holder's public key) and to create the session keys which are used to generate a MAC—the process that Stambler unsuccessfully attempted to prove in Delaware meets the "generating a VAN" limitation in his claims. Stambler's infringement contentions in this case demonstrate that the digital certificates accused today still perform the same SSL-related functions as they did in 2003, and play the same role in Stambler's infringement theory—they are used to generate the session keys used for authentication. *See, e.g.*, Stambler's '148 Patent Infringement Contentions, *passim* (Ex. P); *see also* Comparison Chart of Stambler's Infringement Contentions and the Trial Testimony in the Delaware Action (Ex. S). Stambler's claims should therefore be barred under the *Kessler* doctrine.

D. The *Kessler* Doctrine Extends To This Case

1. *Kessler* Is Intended To Be Broadly Applied

Stambler previously argued—incorrectly—that the *Kessler* doctrine is narrow. *See* Opposition to Motion to Stay at 9. To the contrary, the *Kessler* doctrine has sufficient breadth to ensure that prior judgments against patent holders are given full effect, and to avoid needless re-litigation. *See MGA, Inc.*, 827 F.2d at 734 ("[T]he *Kessler* doctrine, which in its effect may be compared to defensive collateral estoppel, [applies] to give preclusive effect to the issue of noninfringement of the [patent-in-suit] by the accused machines."); c*f. Studiengesellschaft*, 675 F. Supp. at 188 ("The exigencies of litigation demand that at some point there be an end to litigation of a particular issue. . . . Relitigation of infringement issues already decided not only forces producers and sellers of products to divert their resources away from productive uses in favor of repetitious litigation but also hampers their ability to effectively and efficiently produce

and market their products."). The narrow view of *Kessler* urged by Stambler would permit inconsistent decisions and prolonged, multiple litigations. *See General Chemical Co. v. Standard Wholesale Phosphate & Acid Works, Inc.*, 101 F.2d 178, 181 (4th Cir. 1939) ("To hold that [the patentee] is bound by the judgment in suits against other parties with respect to the same subject matter, does him no injustice and prevents unseemly conflict of decision and useless prolonging of a controversy which has been decided against him by the court.").

2. The Accused Product and the Previously Adjudicated Noninfringing Product Need Not Be Absolutely Identical for the *Kessler* Doctrine to Apply

Stambler also incorrectly argues that the *Kessler* doctrine only applies to accused products that are "identical" in every way to the previously exonerated products. *See* Opposition to Motion to Stay at 2. To the contrary, *Kessler* explicitly prohibited further litigation against any customer "on account of his use of the same *kind* of Kessler cigar lighter which had been passed on in the previous case." *See id.* at 288 (emphasis added). In any event, the products here are "identical" with respect to the parts that Stambler alleges to cause infringement; the difference between the old certificates and the new ones does not relate in any way to Stambler's assertions.

Kessler recognizes that "[i]f rights between litigants are once established by the final judgment of a court of competent jurisdiction those rights must be recognized in every way, and wherever the judgment is entitled to respect." *Kessler*, 206 U.S. at 289. The Federal Circuit has stated that the *Kessler* doctrine creates "'the right to have that which [a court has determined a manufacturer] lawfully produces freely bought and sold without restraint or interference.'" *MGA, Inc.*, 827 F.2d at 734 (quoting *Rubber Tire Wheel Co.*, 232 U.S. 413). Whether the accused product is absolutely "identical" to the prior product is not dispositive. *Cf. Studiengesellschaft*, 675 F. Supp. at 188 (focusing, in the collateral estoppel context on whether

the litigated issues are similar, not necessarily the particular products). In other words, Kessler's lighters would have been protected from further claims of infringement even if they were not strictly "identical" to the prior lighters adjudicated not to infringe, provided that they were substantially the same in every aspect relevant to the asserted patent claim. *See Kessler*, 206 U.S. at 288 (basing its decision in equity and noting that the trial court had "conclusively decreed the right of Kessler to manufacture and sell his manufactures free from all interference from Eldred by virtue of the Chambers patent"). In light of the finding of non-infringement in favor of VeriSign in the Delaware Action, and the infringement allegations made by Stambler in this action, application of the *Kessler* doctrine is appropriate and warranted here.

Conclusion

This case involves claims and issues that have previously been litigated. Stambler presented claims accusing VeriSign Digital Certificates as used in SSL version 3.0 to a Delaware jury and lost. Not only does the present action risk conflicting judicial decisions, it is fundamentally unfair to allow Stambler to re-raise those very claims and burden JPMorgan with litigating this action. For these reasons, and those described above, JPMorgan respectfully requests that this Court find that Stambler is precluded from asserting his claims against JPMorgan.

Dated: September 2, 2009

Respectfully submitted,

By: */s/ Mark Matuschak*

David J. Beck
State Bar No. 00000070
BECK, REDDEN & SECREST, L.L.P.
1221 McKinney Street, Suite 4500
Houston, Texas 77010-2010
Telephone: (713) 951-3700
Facsimile: (713) 951-3720
Email: dbeck@brsfirm.com

Michael E. Richardson
State Bar No. 24002838
BECK, REDDEN & SECREST, L.L.P.
1221 McKinney St., Suite 4500
Houston, Texas 77010-2010
Telephone: (713) 951-3700
Facsimile: (713) 951-3720
Email: mrichardson@brsfirm.com

Mark G. Matuschak (*admitted pro hac vice*)
Gregory P. Teran (*admitted pro hac vice*)
Donald R. Steinberg (*admitted pro hac vice*)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6453
Facsimile: (617) 526-5000
Email: mark.matuschak@wilmerhale.com
Email: gregory.teran@wilmerhale.com
Email: donald.steinberg@wilmerhale.com

Mark D. Selwyn (*admitted pro hac vice*)
WILMER CUTLER PICKERING
HALE AND DORR LLP
1117 S. California Avenue
Palo Alto, CA 94304
Telephone: (650) 858-6031
Facsimile: (650) 858-6100
Email: mark.selwyn@wilmerhale.com

Kate Hutchins (*admitted pro hac vice*)
WILMER CUTLER PICKERING
HALE AND DORR LLP
399 Park Avenue
New York, NY 10022
Telephone: (212) 295-6414
Facsimile: (212) 230-8888
Email: kate.hutchins@wilmerhale.com

ATTORNEYS FOR DEFENDANTS JPMORGAN CHASE & CO. AND JPMORGAN CHASE BANK, NATIONAL ASSOCIATION

CERTIFICATE OF SERVICE

I hereby certify that counsel of record who are deemed to have consented to electronic service in the above-referenced case are being served this 2nd day of September, 2009, with a copy of the above document via the court's CM/ECF system per Local Rule CV-5(a)(3).

/s/ Michael E. Richardson
Michael E. Richardson